Storage Area Network (SAN) Checklist
for
Sharing Peripherals Across the Network
Security Technical Implementation Guide
Version 1 Release 1

06 Janauary 2006

Developed by DISA for the DOD

Database Reference Number: _____

Database entered by: _____ Date: _____

Technical Q/A by: _____Date: _____

Final Q/A by: _____ Date: _____

CAT I: _____

CAT II: _____

CAT III: _____

CAT IV: _____

Total: _____

FOUO UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Enclave Reviewer				**Phone**	
Previous SRR	Y N	**Date of Previous SRR**		**S01 Available**	Y N
Number of Current Open Findings					

Site Name	
Address	
Phone	

Position	**Name**	**Phone Number**	**Email**	**Area of Responsibility**
IAM				
IAO				

SAN03.001.00 CAT: 1 Zoning is not used to protect the SAN.

8500.2 IA Control: ECCD-1: ECCD-2 Category: 2.1 - Object Permissions

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability Zoning is not used to protect the SAN..

Vulnerability Discussion: Zoning is an efficient method of managing, partitioning, and controlling pathways to and from storage devices on the SAN fabric; as a result, storage resources are maximized, and data integrity and data security are maintained.
The IAO/NSO will ensure that zoning is used to protect the SAN.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN03.001.00: The reviewer with the assistance of the IAO/NSO, verify that zoning is used to protect the SAN

Fix(es): SPAN SAN03.001.00: Develop a zone topography, from the topography create a plan to implement zoning, obtain CM approval of the plan and then, following the plan, reconfigure the SAN to support zoning.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN03.002.00 CAT: 2 Hard zoning is not used to protect the SAN.

8500.2 IA Control: ECCD-1: ECCD-2 Category: 2.1 - Object Permissions

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability Hard zoning is not used to protect the SAN.

Vulnerability Discussion: Hard zoning, as apposed to soft zoning, is enforced by the port hardware level and is harder to subvert than soft zoning which is controlled by software.
The IAO/NSO will ensure that hard zoning is used to protect the SAN.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN03.002.00: The reviewer, with the assistance of the IAO/NSO, will verify that hard zoning is used to protect the SAN.

Fix(es): SPAN SAN03.002.00: If zoning has not been implemented, develop a zone topography, from the topography create a plan to implement hard zoning, obtain CM approval of the plan and then, following the plan, reconfigure the SAN to support hard zoning.

If zoning has been implemented develop a plan to migrate to hard zoning, obtain CM approval of the plan and then, following the plan, reconfigure the SAN to support hard zoning.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN03.003.00 CAT: 2 The default zone visibility is not set to "none"

8500.2 IA Control: ECCD-1: ECCD-2 Category: 2.1 - Object Permissions

Condition(s): SANS Switch: SANS Storage Device

Target(s): SANS Storage Device; SANS Switch

Vulnerability The default zone visibility setting is not set to “none”.

Vulnerability Discussion: If the default zone visibility setting is set to "none", new clients brought into the SAN will not be allowed access to any SAN zone they are not explicitly placed into.
The IAO/NSO will ensure that the default zone visibility setting, if available, is set to “none”.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN03.003.00: Reviewer with the assistance of the IAO/NSO, verify that the default zone visibility setting is set to “none”.. If this setting is not available mark this check as N/A.

Fix(es): SPAN SAN03.003.00: Locate all clients that have not been explicitly placed into a zone. Create a plan to explicitly place these clients into the correct zone(s) and after doing so the plan will include the modification of the default zone visibility setting to “none”. Obtain CM approval of the plan and then, following the plan, reconfigure the SAN to allow for the default zone visibility setting to be set to “none”.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN03.004.00 CAT: 3 Hard zoning, using Port World Wide Names (PWWN)

8500.2 IA Control: ECCD-1: ECCD-2 Category: 2.1 - Object Permissions

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability Hard zoning, using Port World Wide Names (PWWN), is not used to protect the SAN.

Vulnerability Discussion: Hard zoning, as apposed to soft zoning, is enforced by the port hardware level and is harder to subvert than soft zoning which is controlled by software.
The IAO/NSO will ensure that hard zoning, using Port World Wide Names (PWWN), is used to protect the SAN.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN03.004.00: The reviewer with the assistance of the IAO/NSO, verify that hard zoning, using Port World Wide Names (PWWN), is used to protect the SAN.

Fix(es): SPAN SAN03.004.00: Develop a plan to migrate the SAN to Hard Zoning, obtain CM approval of the plan, and the implement the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN03.005.00 CAT: 1 The zoning tables on all affected HBAs reset

8500.2 IA Control: DCSS-1: DCSS-2 Category: 2.1 - Object Permissions

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability The zoning tables on all affected HBAs are not reset (force a state change update) after making zoning changes.

Vulnerability Discussion: The HBA on the initiating devices also store a copy of the ACL. It is possible for the zoning information stored on the HBA to include old addresses, which are no longer allowed in the newly established zoning rules. The HBA's memory is non-persistent, thus a good practice is to force a state change update in the affected HBAs immediately after making zoning changes.
The IAO/NSO will ensure that the zoning tables on all affected HBAs are reset (force a state change update) after making zoning changes.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN03.005.00: The reviewer will interview the IAO/NSO to validate that the zoning tables on all affected HBAs are reset (force a state change update) after making zoning changes. This reset is a manual activity so the interview is to find that the IAO/NSO is aware of this requirement and does it.

Fix(es): SPAN SAN03.005.00: Develop and document a procedure to reset (force a state change update) all effected HBAs whenever SAN zoning configuration changes are made.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.001.00 CAT: 3 SAN devices not added to the site SSAA

8500.2 IA Control: DCID-1 Category: 12.2 - SSAA Doccumentation

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability SAN devices are not added to the site System Security Authorization Agreement (SSAA).

Vulnerability Discussion: All hardware and software will be entered into the SSAA. This gives a central location where it can be shown that all interested parties have reviewed the impact on their security posture and approved the implementation of the SAN.
The IAO/NSO will ensure that SAN devices are added to the site System Security Authorization Agreement (SSAA).

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.001.00: The reviewer will interview the IAO/NSO to validate that SAN devices are added to the site System Security Authorization Agreement (SSAA).

Fix(es): SPAN SAN04.001.00: Update the SSAA following the SSAA review and acceptance procedures to include the SAN.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.002.00 CAT: 2 Compliance with Network Infrastructure and Enclave

8500.2 IA Control: DCCS-1: DCCS-2 Category: 12.7 - Self-Assessment

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability The SANs are not compliant with overall network security architecture, appropriate enclave, and data center security requirements in the Network Infrastructure STIG and the Enclave STIG

Vulnerability Discussion: Inconsistencies with the Network Infrastructure STIG, the Enclave STIG, and the SAN implementation can lead to the creation of vulnerabilities in the network or the enclave.
The IAO/NSO will ensure that SANs are compliant with overall network security architecture, appropriate enclave, and data center security requirements in the Network Infrastructure STIG and the Enclave STIG.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.002.00: The reviewer will interview the IAO/NSO to validate that SANs are compliant with overall network security architecture, appropriate enclave, and data center security requirements in the Network Infrastructure STIG and the Enclave STIG

Fix(es): SPAN SAN04.002.00: Perform a self assessment with the Network Infrastructure checklist and the Enclave checklist or schedule a formal review with FSO.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.003.00 CAT: 2 All security related patches are not installed.

8500.2 IA Control: VIVM-1 Category: 3.1 - Security Patches

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability All security related patches are not installed.

Vulnerability Discussion: Failure to install security related patches leaves the SAN open to attack by exploiting known vulnerabilities.
The IAO/NSO will ensure that all security-related patches are installed.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.003.00: The reviewer will, with the assistance of the IAO/NSO, verify that all security related patches are installed.

Fix(es): SPAN SAN04.003.00: After verifying that the patches do not adversely impact the production SAN, create a plan for installing the patches on the SAN, obtain CM approval of the plan, and implement the plan installing the patches.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.004.00 CAT: 2 Component Compliance with applicable STIG

8500.2 IA Control: DCCS-1: DCCS-2 Category: 12.7 - Self-Assessment

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability Prior to installing SAN components (servers, switches, and management stations) onto the DOD network infrastructure, components are not configured to meet the applicable STIG requirements.

Vulnerability Discussion: Many SAN components (servers, switches, management stations) have security requirements from other STIGs. It will be verified that all requirement are complied with.
The IAO/NSO will ensure that prior to installing SAN components (servers, switches, and management stations) onto the DOD network infrastructure, components are configured to meet the applicable STIG requirements.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.004.00: The reviewer will interview the IAO/NSO and view VMS to verify that prior to installing SAN components (servers, switches, and management stations) onto the DOD network infrastructure, components are configured to meet the applicable STIG requirements.

Fix(es): SPAN SAN04.004.00: Perform a self assessment using the applicable checklists or scripts on any component device that has not been reviewer or request a formal review from FSO.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.005.00 CAT: 2 Servers and hosts OS STIG Requirements

8500.2 IA Control: DCCS-1: DCCS-2 Category: 12.7 - Self-Assessment

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability Servers and other hosts are not compliant with applicable Operating System (OS) STIG requirements.

Vulnerability Discussion: SAN servers and other hosts are hardware software combinations that actually run under the control of a native OS found on the component. This OS may be UNIX, LNIX, Windows, etc. The underlying OS must be configured to be compliant with the applicable STIG to ensure that they do not insert known vulnerabilities into the DOD network infrastructure.
The IAO/NSO will ensure that servers and other hosts are compliant with applicable Operating System (OS) STIG requirements.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.005.00: The reviewer will interview the IAO/NSO and view the VMS to verify that servers and other hosts are compliant with applicable Operating System (OS) STIG requirements.

Fix(es): SPAN SAN04.005.00: Perform a self assessment using the applicable OS checklists or scripts on any server or host in the SAN that has not been reviewer or request a formal review from FSO.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.006.00 CAT: 1 Anti-virus on servers and host.

8500.2 IA Control: ECVP-1 Category: 14.7 - Antivirus

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability Vendor supported, DOD approved, anti-virus software is not installed and configured on all SAN servers in accordance with the applicable operating system STIG on SAN servers and management devices and kept up-to-date with the most recent virus definition tables.

Vulnerability Discussion: The SAN servers and other hosts are subject to virus and worm attacks as are any systems running an OS. If the anti-virus software is not installed or the virus definitions are not maintained on these systems, this could expose the entire enclave network to exploits of known vulnerabilities.
The IAO/NSO will ensure that vendor supported, DOD approved, anti-virus software is installed and configured on all SAN servers in accordance with the applicable operating system STIG on SAN servers and management devices and kept up-to-date with the most recent virus definition tables.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.006.00: The reviewer will verify that vendor supported, DOD approved, anti-virus software is installed and configured on all SAN servers in accordance with the applicable operating system STIG on SAN servers and management devices and kept up-to-date with the most recent virus definition tables. If an OS review has reciently been completed verify that the anti-virus check was not a finding. Otherwise perform a manual check as described in the applicable OS checklist.

Fix(es): SPAN SAN04.006.00: Install and correctly configure a DOD approved anti-virus.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.007.00 CAT: 2 SAN Topology Drawing

8500.2 IA Control: DCHW-1 Category: 12.9 - Documentation

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability A current drawing of the site's SAN topology that includes all external and internal links, zones, and all interconnected equipment is not being maintained.

Vulnerability Discussion: A drawing of the SAN topology gives the IAO and other interested individuals a pictorial representation of the SAN. This can be helpful in diagnosing potential security problems.
The IAO/NSO will maintain a current drawing of the site's SAN topology that includes all external and internal links, zones, and all interconnected equipment.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SA04.007.00: The reviewer will interview the IAO/NSO and view the drawings supplied to verify that a current drawing of the site's SAN topology that includes all external and internal links, zones, and all interconnected equipment.

Fix(es): SPAN SAN04.007.00: Create drawing of the site's SAN topology that includes all external and internal links, zones, and all interconnected equipment.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.008.00 CAT: 2 Physical Access to SAN Network Devices

8500.2 IA Control: PECF-1: PECF-2 Category: 5.9 - Device Locations

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability All the network level devices interconnected to the SAN are not located in a secure room with limited access.

Vulnerability Discussion: If the network level devices are not located in a secure area they can be tampered with which could lead to a denial of service if the device is powered off or sensitive data can be compromised by a tap connected to the device.
The IAO/NSO will ensure that all the network level devices interconnected to the SAN are located in a secure room with limited access.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.008.00: The reviewer will interview the IAO/NSO and view the network level devices to verify whether they are located in a secure room with limited access.

Fix(es): SPAN SAN04.008.00: Develop a plan to move the network level devices to a location/room where the can be physically secured in a manner appropriate to the classification level of the data the handle. Obtain CM approval of the plan and then implement the plan moving the devices.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.009.00 CAT: 2 SAN Fabric Switch User Accounts with Passwords

8500.2 IA Control: IAIA-1: IAIA-2 Category: 1.3 - Identity Management

Condition(s): SANS Switch: SANS Storage Device

Target(s): SANS Storage Device; SANS Switch

Vulnerability Individual user accounts with passwords are not set up and maintained for the SAN fabric switch.

Vulnerability Discussion: Without identification and authentication unauthorized users could reconfigure the SAN or disrupt its operation by logging in to the fabric switch and executing unauthorized commands.
The IAO/NSO will ensure individual user accounts with passwords are set up and maintained for the SAN fabric switch in accordance with the guidance contained in Appendix B, CJCSM and the Network Infrastructure STIG.

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SA04.009.00: The reviewer, with the assistance of the IAO/NSO, will verify that individual user accounts with passwords are set up and maintained for the SAN fabric switch.

Fix(es): SPAN SA04.009.00: Develop a plan to reconfigure the SAN fabric switch to require user accounts and passwords. This plan also needs to include the creation and distribution of user accounts and passwords for each administrator who requires access to the SAN fabric switch. Obtain CM approval of the plan and then implement the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.010.00 CAT: 3 Sensitive Data in Transit Encryption

8500.2 IA Control: ECNK-1 Category: 8.1 - Encrypted Data in Transit

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability All fabric switches for SANs that process sensitive information are not configured to use a FIPS 140-1/2 validated algorithm to encrypt switch-to-switch communications.

Vulnerability Discussion: It is necessary to protect the confidentiality of sensitive data in transit over a network that is used to transmit other sensitive data that has a differing need-to-know criteria.
The IAO/NSO will configure all fabric switches to use a FIPS 140-1/2 validated algorithm to encrypt switch-to-switch communications for SANs that process sensitive information.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.010.00: The reviewer will, with the assistance of the IAO/NSO, verify that all fabric switches are configured to use a FIPS 140-1/2 validated algorithm to encrypt switch-to-switch communications for SANs that process sensitive information.

Fix(es): SPAN SAN04.010.00: Develop a plan to reconfigure the SAN fabric switches to use FIPS-140-1/2 validated algorithms to encrypt switch-to-switch communications for SANs that process sensitive information. Obtain CM approval for the plan and then implement the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.011.00 CAT: 3 SAN Switch encryption and DOD PKI

8500.2 IA Control: ECNK-1: IAIA-1: IAIA-2 Category: 1.3 - Identity Management

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability The fabric switches are not protected by encryption and DOD PKI and/or that the manufacturer's default keys have not been changed prior to attaching to the SAN Fabric for SANs processing sensitive information..

Vulnerability Discussion: Failure to provide encryption for SAN switches that handle sensitive data can lead to the compromise of sensitive data. DOD PKI will supplies better protection from malicious attacks than userid/password authentication and should be used anytime it is feasible. If manufactures default keys are not changed prior to connection to the network the switch will be vulnerable to malicious attacks by individuals who know these keys.
The IAO/NSO will ensure that fabric switches are protected by encryption and DOD PKI and that the manufacturer's default keys are changed prior to attaching to the SAN Fabric for SANs processing sensitive information.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.011.00: The reviewer will, with the assistance of the IAO/NSO, verify that fabric switches are protected by encryption and DOD PKI and that the manufacturer's default keys are changed prior to attaching to the SAN Fabric for SANs processing sensitive information.

Fix(es): SPAN SAN04.011.00: Develop a plan to implement encryption, DOD PKI and change the manufacturers default keys. Obtain CM approval for the plan and then execute the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.012.00 CAT: 2 SAN Network Management Ports Fabric Switch

8500.2 IA Control: DCBP-1 Category: 14.4 - Unneeded Ports, Protocols, Hardware, and Services

Condition(s): SANS Switch

Target(s): SANS Switch

Vulnerability Network management ports on the SAN fabric switches except those needed to support the operational commitments of the sites are not disabled.

Vulnerability Discussion: Enabled network management ports that are not required expose the SAN fabric switch and the entire network to unnecessary vulnerabilities. By disabling these unneeded ports the exposure profile of the device and network is diminished.
The IAO/NSO will disable all network management ports on the SAN fabric switches except those needed to support the operational commitments of the sites.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.012.00: The reviewer will, with the assistance of the IAO/NSO, verify that all network management ports on the SAN fabric switches are disabled except those needed to support the operational commitments of the sites.

Fix(es): SPAN SAN04.012.00: Develop a plan to locate and disable all network management ports that are not required to support the operational commitments of the sites. Obtain CM approval of the plan and then execute the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.013.00 CAT: 2 SAN management out-of-band or direct connect

8500.2 IA Control: DCBP-1 Category: 14.5 - Physical Layer Security

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability SAN management is accomplished using the out-of-band or direct connection method.

Vulnerability Discussion: Removing the management traffic from the production network diminishes the security profile of the SAN servers by allowing all the management ports to be closed on the production network.
The IAO/NSO will ensure that SAN management is accomplished using the out-of-band or direct connection method.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.013.00: The reviewer will interview the IAO and view the SAN network drawings provided.

Fix(es): SPAN SAN04.013.00: Develop a plan to migrate the SAN management to an out-of-band network or a direct connect method. Obtain CM approval for the plan and implement the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.014.00 CAT: 3 Management Console to SAN Fabric DOD PKI protected

8500.2 IA Control: IAIA-1: IAIA-2 Category: 1.2 - PKI

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability Communications from the management console to the SAN fabric are not protected using DOD PKI.

Vulnerability Discussion: Using DOD PKI authentication between the SAN management console and the fabric enhances the security of the communications carrying privileged functions. It is harder for an unauthorized management console to take control of the SAN.
The IAO/NSO will ensure that communications from the management console to the SAN fabric are protected using DOD PKI.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.014.00: The reviewer will, with the assistance of the IAO/NSO, verify that communications from the management console to the SAN fabric are protected using DOD PKI.

Fix(es): SPAN SAN04.014.00: Develop a plan to migrate to the use of DOD PKI authentication between the SAN management console and the SAN fabric. Obtain CM approval of the plan and implement the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.015.00 CAT: 3 Default PKI keys

8500.2 IA Control: IAIA-1: IAIA-2 Category: 1.2 - PKI

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability The manufacturer’s default PKI keys have not been changed prior to attaching the switch to the SAN Fabric.

Vulnerability Discussion: If the manufacturer's default PKI keys are allowed to remain active on the device, it can be accessed by a malicious individual with access to the default key.
The IAO/NSO will ensure that the manufacturer’s default PKI keys are changed prior to attaching the switch to the SAN Fabric.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.015.00: The reviewer will, with the assistance of the IAO/NSO, verify that the manufacturer’s default PKI keys have been changed prior to attaching the switch to the SAN Fabric.

Fix(es): SPAN SAN04.015.00: Depending on the functionality allowed by the device, develop a plan remove, disable or change the manufacturer’s default PKI certificate so that it cannot be used for identification and authorization. Obtain CM approval for the plan and implement the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.016.00 CAT: 3 FIPS 140-1/2 for management to fabric.

8500.2 IA Control: ECNK-1 Category: 8.1 - Encrypted Data in Transit

Condition(s): SANS Switch: SANS Storage Device

Target(s): SANS Storage Device; SANS Switch

Vulnerability The SAN is not configured to use FIPS 140-1/2 validated encryption algorithm to protect management-to-fabric communications.

Vulnerability Discussion: The communication between the SAN management consol and the SAN fabric carries sensitive privileged configuration data. This data's confidentiality will be protected with FIPS 140-1/2 validate algorithm for encryption. Configuration data could be used to create a denial of service by disrupting the SAN fabric.
The storage administrator will configure the SAN to use FIPS 140-1/2 validated encryption algorithm to protect management-to-fabric communications.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.016.00: The reviewer will, with the assistance of the storage administrator, verify that the SAN is configured to use FIPS 140-1/2 validated encryption algorithm to protect management-to-fabric communications.

Fix(es): SPAN SA04.016.00: Develop a plan to implement FIPS-140-1/2 validated encryption to protect management-to-fabric communications. Obtain CM approval of the plan and execute the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.017.00 CAT: 1 Password SAN Management Console and Ports

8500.2 IA Control: IAIA-1: IAIA-2 Category: 1.3 - Identity Management

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability All SAN management consoles and ports are not password protected.

Vulnerability Discussion: Without password protection malicious users can create a denial of service by disrupting the SAN or allow the compromise of sensitive date by reconfiguring the SAN topography.
The IAO/NSO will ensure that all SAN management consoles and ports are password protected.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.017: The reviewer will, with the assistance of the IAO/NSO, verify that all SAN management consoles and ports are password protected.

Fix(es): SPAN SAN04.017.00: Develop a plan for implementing password protection on the SAN's management consoles and ports. Obtain CM approval of the plan and execute the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.018.00 CAT: 1 Default SAN Management Software Password

8500.2 IA Control: IAIA-1: IAIA-2 Category: 1.3 - Identity Management

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability The manufacturer's default passwords have not been changed for all SAN management software.

Vulnerability Discussion: The changing of passwords from the default value blocks malicious users with knowledge of the default passwords for the manufacturer's SAN Management software from creating a denial of service by disrupting the SAN or reconfigure the SAN topology leading to a compromise of sensitive data.
The IAO/NSO will ensure that the manufacturer's default passwords are changed for all SAN management software.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.018.00: The reviewer will, with the assistance of the IAO/NSO, verify that the manufacturer's default passwords have been changed for all SAN management software.

Fix(es): SPAN SAN04.018.00: Develop a plan to change manufacturer's default passwords for all SAN management software. Obtain CM approval of the plan and implement the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.019.00 CAT: 1 SAN Fabric Zoning List Deny-By-Default

8500.2 IA Control: DCBP-1 Category: 2.1 - Object Permissions

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability The SAN fabric zoning lists are not based on a policy of Deny-by-Default with blocks on all services and protocols not required on the given port or by the site.

Vulnerability Discussion: By using the Deny-by-Default based policy, any service or protocol not required by a port and overlooked in the zoning list will be denied access. If Deny-by-Default based policy was not used any overlooked service or protocol not required by a port could have access to sensitive data compromising that data.
The IAO/NSO will ensure that SAN fabric zoning lists are based on a policy of Deny-by-Default with blocks on all services and protocols not required on the given port or by the site.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.019.00: The reviewer will, with the assistance of the IAO/NSO, verify that SAN fabric zoning lists are based on a policy of Deny-by-Default with blocks on all services and protocols not required on the given port or by the site.

Fix(es): SPAN SAN04.019.00: Develop a plan to identify all services and protocols needed by each port in the SAN, modify the routing lists to enforce a Deny-by-Default policy and allow only the identified services and protocols on each port that requires them. Obtain CM approval for the plan and implement the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.020.00 CAT: 3 Logging Failed Access to Port, Protocols, Services

8500.2 IA Control: ECAR-1: ECAR-2: ECAR-3 Category: 10.2 - Content Configuration

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability Attempts to access ports, protocols, or services that are denied are not logged..

Vulnerability Discussion: Logging or auditing of failed access attempts is a necessary component for the forensic investigation of security incidents. Without logging there is no way to demonstrate that the access attempt was made or when it was made. Additionally a pattern of access failures cannot be demonstrated to assert that an intended attack was being made as apposed to an accidental intrusion.
The IAO/NSO will ensure that all attempts to any port, protocol, or service that is denied are logged.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.020.00: The reviewer will, with the assistance of the IAO/NSO, verify that all attempts to any port, protocol, or service that is denied are logged.

Fix(es): SPAN SAN04.020.00: Develop a plan to implement the logging of failed or rejected ports, protocols or services requests. The plan should include a projection of the storage requirements of the logged events. Obtain CM approval of the plan and execute it.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.021.00 CAT: 2 SNMP usage and configuration.

8500.2 IA Control: DCBP-1 Category: 14.2 - Protocol Security

Condition(s): SANS Switch: SANS Storage Device

Target(s): SANS Storage Device; SANS Switch

Vulnerability Simple Network Management Protocol (SNMP) is used and it is not configured in accordance with the guidance contained in the Network Infrastructure STIG.

Vulnerability Discussion: There are vulnerabilities in some implementations and some configurations of SNMP. Therefore if SMPT is used the guidelines found in the Network Infrastructure STIG in selecting a version of SNMP to use and how to configure it will be followed.
If Simple Network Management Protocol (SNMP) is used, the IAO/NSO will ensure it is configured in accordance with the guidance contained in the Network Infrastructure STIG.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.021.00: With the assistance of the IAO/NSO, verify that if Simple Network Management Protocol (SNMP) is used, it is configured in accordance with the guidance contained in the Network Infrastructure STIG section 5.1.2.

Fix(es): SPAN SAN04.021.00: Develop a plan to implement SNMP that is compliant with the Network Infrastructure STIG. Obtain CM approval and execute the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.022.00 CAT: 1 Authorized IP Addresses allowed for SNMP

8500.2 IA Control: DCBP-1 Category: 14.2 - Protocol Security

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability Unauthorized IP addresses are allowed Simple Network Management Protocol (SNMP) access to the SAN devices.

Vulnerability Discussion: SNMP, by virtue of what it is designed to do, can be a large security risk. Because SNMP can obtain device information and set device parameters, unauthorized users can cause damage. Restricting IP address that can access SNMP on the SAN devices will further limit the possibility of malicious access being made.
The IAO/NSO will ensure that only authorized IP addresses are allowed Simple Network Management Protocol (SNMP) access to the SAN devices.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.022.00: The reviewer will, with the assistance of the IAO/NSO, verify that only authorized IP addresses are allowed Simple Network Management Protocol (SNMP) access to the SAN devices. This can be done with by checking the ACLs for the SAN device ports.

Fix(es): SPAN SAN04.022.00: Develop a plan to restrict SNMP access to SAN devices to authorized IP addresses. Obtain CM approval for the plan and implement the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.023.00 CAT: 2 Only Internal Network SNMP Access to SAN

8500.2 IA Control: EBRP-1 Category: 2.1 - Object Permissions

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability The IP addresses of the hosts permitted SNMP access to the SAN management devices do not belong to the internal network.

Vulnerability Discussion: SNMP, by virtue of what it is designed to do, can be a large security risk. Because SNMP can obtain device information and set device parameters, unauthorized users can cause damage. Therefore access to a SAN device from an IP address outside of the internal network will not be allowed.
The IAO/NSO will ensure IP addresses of the hosts that are permitted SNMP access to the SAN management devices belong to the internal network.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.023.00: The reviewer will, with the assistance of the IAO/NSO, verify that the IP addresses of the hosts permitted SNMP access to the SAN management devices belong to the internal network. The ACLs for the SAN ports should be checked.

Fix(es): SPAN SAN04.023.00: Develop a plan to restrict SNMP access to SAN devices to only internal network IP addresses. Obtain CM approval of the plan and implement the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.024.00 CAT: 3 Fibre Channel network End-User Platform Restricted

8500.2 IA Control: DCBP-1 Category: 2.1 - Object Permissions

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability End-user platforms are directly attached to the Fibre Channel network or access storage devices directly.

Vulnerability Discussion: End-user platforms should only be connected to servers that run applications that access the data found on the SAN devices. SANs do not supply a robust user identification and authentication platform. They depend on the servers and applications to authenticate the users and restrict access to users as required.
The IAO/NSO will ensure that end-user platforms are not directly attached to the Fibre Channel network and may not access storage devices directly.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.024.00: The reviewer will, with the assistance of the IAO/NSO, verify that end-user platforms are not directly attached to the Fibre Channel network and may not access storage devices directly. If the SAN is small with all of its components collocated, this can be done by a visual inspection but in most cases the reviewer will have to check the SAN network drawing.

Fix(es): SPAN SAN04.024.00: Develop a plan to remove end-user platforms from the SAN. Obtain CM approval for the plan and implement the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN04.025.00 CAT: 2 SAN Fixed IP Required.

8500.2 IA Control: DCBP-1 Category: 14.3 - Network Device Configuration

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability SAN components are not configured with fixed IP addresses.

Vulnerability Discussion: Without fixed IP address filtering or restricting of access based on IP addressing will not function correctly allowing unauthorized access to SAN components or creating a denial of service by blocking legitimate traffic from authorized components. The storage administrator will ensure that all SAN components are configured to use static IP addresses.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN04.25.00: The reviewer with the assistance of the SA will verify that all SAN components are configured with fixed IP addresses.

Fix(es): SPAN SAN04.025.00: Configure all SAN components to have fixed IP addresses.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

SAN05.001.00 CAT: 2 Backup of critical SAN Software and configurations

8500.2 IA Control: COSW-1 Category: 13.4 - Backup & Recovery

Condition(s): SANS Storage Device: SANS Switch

Target(s): SANS Storage Device; SANS Switch

Vulnerability Fabric switch configurations and management station configuration are not archived and/or copies of the operating system and other critical software for all SAN components are not stored in a fire rated container or are not collocated with the operational software.

Vulnerability Discussion: .Backup and recovery procedures are critical to the security and availability of the SAN system. If a system is compromised, shut down, or otherwise not available for service, this could hinder the availability of resources to the warfighter.
The IAO/NSO will ensure that all fabric switch configurations and management station configuration are archived and copies of the operating system and other critical software for all SAN components are stored in a fire rated container or otherwise not collocated with the operational software.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN05.001.00: The reviewer will interview the IAO/NSO and view the stored information to verify that all fabric switch configurations and management station configuration are archived and copies of the operating system and other critical software for all SAN components are stored in a fire rated container or otherwise not collocated with the operational software.

Fix(es): SPAN SAN05.001.00: Develop a plan that will ensure that all fabric switch configurations and management station configuration are archived and copies of the operating system and other critical software for all SAN components are stored in a fire rated container or otherwise not collocated with the operational software. Obtain CM approval for the plan and implement the plan.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes: